

**IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN**

MICHAEL MEEKS , on behalf of himself and all others similarly situated, v. ONETOUCHPOINT, INC. , Defendant.	Case No. Judge JURY TRIAL DEMANDED
---	---

CLASS ACTION COMPLAINT

Plaintiff Michael Meeks (hereinafter known as “Plaintiff” or “Meeks”), individually and on behalf of all others similarly situated, brings this action against Defendant OneTouchPoint, Inc. (hereinafter known as “Defendant”), a Wisconsin corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach (“Data Breach”) on Defendant’s network that resulted in unauthorized access to patient data. As a result of the Data Breach, Plaintiff and approximately 1,073,316 Class Members¹ suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

¹ <https://apps.web.maine.gov/online/aeviewer/ME/40/0a2e4b99-8e95-4860-b05f-62c239a13993.shtml> (Last visited August 8, 2022).

2. In addition, Plaintiff and Class Members' sensitive personal information—which was entrusted to Defendant, its officials, and its agents—was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes names, addresses, member ID numbers, dates of birth, and Social Security Numbers, (“PII”), and medical and health assessment information, diagnosis codes, and description of services (“PHI”).² The PII and PHI that Defendant collected and maintained will be collectively referred to as the “Private Information.”

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of his and Class Members' Private Information that Defendant collected and maintained, and for Defendant's failure to (1) provide timely and adequate notice to Plaintiff and other Class Members that their Private Information had been subject to the unauthorized access of an unknown third party, and (2) identify precisely what specific type of information was accessed.

5. Defendant maintained the Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

² <https://www.securityweek.com/onetouchpoint-discloses-data-breach-impacting-over-30-healthcare-firms> (Last visited August 8, 2022).

6. Plaintiff and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

9. Plaintiff and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. By his Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

11. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

12. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of implied contract; (iii) unjust enrichment; and (iv) invasion of privacy.

THE PARTIES

13. Plaintiff Michael Meeks is a natural person, resident, and a citizen of the State of Georgia. Meeks has no intention of moving to a different state in the immediate future. Plaintiff Meeks is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Meeks's Private Information and owed him a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Meeks would not have entrusted his Private Information to Defendant had he known that Defendant failed to maintain adequate data security. Plaintiff Meeks's Private Information was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

14. Defendant OneTouchPoint, Inc. is a Wisconsin corporation with its headquarters and principal place of business is located at 1225 Walnut Ridge Dr., Hartland, Wisconsin 53029.

JURISDICTION AND VENUE

15. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds \$5,000,000, exclusive of interest and costs. Plaintiff (and many members of the class) and Defendant are citizens of different states. Plaintiff is a citizen of Georgia. Defendant is a Wisconsin corporation with its headquarters and principal place of business is located at 1225 Walnut Ridge Dr., Hartland, Wisconsin 53029

16. This Court has general personal jurisdiction over Defendant because Defendant's principal place of business is in Hartland, Wisconsin. Defendant and regularly conducts business in Wisconsin.

17. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

DEFENDANT'S BUSINESS

18. Defendant provides printing and mailing services for client companies within the United States. For business purposes, Defendant received the information of individuals from customer organizations which Defendant utilized to conduct mailings on behalf of their customers.

19. On information and belief, in the ordinary course of printing and mailing items on behalf of its customer organizations, Defendant maintains the Private Information of patients and customers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Medication information,
- Health insurance information,
- Photo identification;

- Employment information, and;
- Other information that Defendant may deem necessary to provide care.

20. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its customers, Defendant, upon information and belief, promises to, among other things: keep customers' protected health information (PHI) private; comply with healthcare industry standards related to data security and Private Information; inform customers and patients of its legal duties and comply with all federal and state laws protecting customers' and patients' Private Information; only use and release customers' Private Information for reasons that relate to medical care and treatment; provide adequate notice to customers if their Private Information is disclosed without authorization; and adhere to the terms outlined in its Privacy Policy.³

21. As a condition of printing and mailing services for its customer organizations, Defendant requires that its customers entrust it with Private Information of Plaintiff and Class Members.

22. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

23. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

24. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and

³ <https://1touchpoint.com/privacy-policy>.

securely maintained, to use such Private Information solely for business, printing, and mailing purposes, and to prevent the unauthorized disclosures of the Private Information.

THE CYBERATTACK AND DATA BREACH

25. On April 28, 2022, Defendant discovered encrypted files on certain company computer systems within its network.

26. Through investigation, Defendant determined that its network and servers were subject to a cyber-attack that impacted its network.

27. The investigation determined that files on Defendant's network were accessed by an unauthorized user.

28. Upon information and belief, Plaintiff's and Class Members' Private Information was exfiltrated and stolen in the attack.

29. Defendant worked with "third-party forensic specialists" to determine the scope of the activity of the cyber-attack.

30. Furthermore, the investigation determined that the accessed systems contained Private Information and that was accessible, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

31. The type of Private Information allegedly accessed by the unauthorized actor included includes names, member IDs, and information that was provided during a health assessment.⁴

32. As a result of the Data Breach, Defendant took steps to secure the network, and launched a thorough investigation, with the assistance of third-party experts, to determine the

⁴ <https://apps.web.maine.gov/online/aeviewer/ME/40/0a2e4b99-8e95-4860-b05f-62c239a13993.shtml> (Last visited August 8, 2022).

nature and scope of the incident. The investigation revealed that approximately 1,073,316 individuals were victims of the Data Breach.⁵

33. While Defendant stated in the notice letter that April 28, 2022 was the date the Data Breach was discovered, Defendant did not begin notifying victims until late July 2022 – approximately three months later.

34. Upon information and belief, and based on the type of cyberattack, along with public news reports, it is plausible and likely that Plaintiff's Private Information was stolen in the Data Breach. Plaintiff further believes his Private Information was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of all cybercriminals.

35. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

36. Plaintiff and Class Members provided their Private Information to Defendant's customer organizations with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

37. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

38. In light of recent high profile data breaches at other healthcare partner and provider companies, Defendant knew or should have known that their electronic records and patient and customer Private Information would be targeted by cybercriminals and ransomware attack groups.

⁵ https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

39. Indeed, cyberattacks on medical systems like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”⁶

40. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.⁷

41. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

42. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

43. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any

⁶ *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited June 23, 2021).

⁷ *See Maria Henriquez, Iowa City Hospital Suffers Phishing Attack*, Security Magazine (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack>.

security problems.⁸ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.⁹

44. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

45. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

46. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”)

47. Defendant failed to properly implement basic data security practices.

⁸ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 19, 2022).

⁹ *Id.*

48. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

49. Defendant was at all times fully aware of its obligation to protect the Private Information of its customers and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

50. As shown above, experts studying cyber security routinely identify healthcare providers and their partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

51. Several best practices have been identified that at a minimum should be implemented by companies like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

52. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

53. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

54. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

DEFENDANT'S BREACH

55. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect Private Information of Plaintiff and the Class;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;
- e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;
- f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

- g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- l. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);
- m. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

- n. Failing to adhere to industry standards for cybersecurity as discussed above;
and
- o. Otherwise breaching its duties and obligations to protect Plaintiff's and
Class Members' Private Information.

56. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted Private Information.

57. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

***Cyberattacks and Data Breaches Cause Disruption and
Put Consumers at an Increased Risk of Fraud and Identity Theft***

58. Cyberattacks and data breaches at healthcare associated companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

59. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.¹⁰

60. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient

¹⁰ See Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), <https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks>.

outcomes, generally.¹¹

61. The United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”¹²

62. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims’ identities in order to engage in illegal financial transactions under the victims’ names. Because a person’s identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim’s identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information about a victim’s identity, such as a person’s login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

63. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone

¹¹ See Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at <https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203>.

¹² See U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007). Available at <https://www.gao.gov/new.items/d07737.pdf>.

steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.¹³

64. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

65. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

66. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.¹⁴

67. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

68. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance

¹³ See *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/Steps> (last visited Aug. 9, 2022).

¹⁴ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”¹⁵

69. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

70. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

71. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

72. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

73. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

¹⁵ *See* Federal Trade Commission, *Medical Identity Theft*, <http://www.consumer.ftc.gov/articles/0171-medical-identity-theft> (last visited Jan. 19, 2022).

74. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

75. Private Information can sell for as much as \$363 per record according to the Infosec Institute.¹⁶ PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

76. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.¹⁷ Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.¹⁸ Each of these fraudulent activities is difficult to detect. An individual may not know that his or his Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

77. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

78. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security

¹⁶ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>.

¹⁷ *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (Jan. 19, 2022).

¹⁸ *Id* at 4.

number.”¹⁹

79. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”²⁰

80. Medical information is especially valuable to identity thieves.

81. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just \$1 in 2016 – the same as a Facebook account.²¹ That pales in comparison with the asking price for medical data, which was selling for \$50 and up.²²

82. Because of the value of its collected and stored data, the medical industry has experienced disproportionately higher numbers of data theft events than other industries.

83. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

Plaintiff and Class Members’ Damages

84. To date, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

¹⁹ Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>.

²⁰ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

²¹ See Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), <https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/>.

²² Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>.

85. Defendant has merely offered Plaintiff and Class Members complimentary fraud alert services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

86. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

87. At the least, Plaintiff's name, member ID information, and private information exchanged during health assessments were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

88. Since being notified of the Data Breach, Plaintiff Meeks has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

89. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring his accounts for fraudulent activity.

90. Plaintiff's Private Information was compromised as a direct and proximate result of the Data Breach.

91. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

92. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

93. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

94. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members. Plaintiff has already experienced various phishing attempts by telephone and through electronic mail.

95. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

96. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

97. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendant's customers was intended to be used by Defendant to fund adequate security of Defendant's computer system and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for and agreed to.

98. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their medical accounts and sensitive information for misuse.

99. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- b. Purchasing credit monitoring and identity theft prevention;
- c. Placing “freezes” and “alerts” with reporting agencies;
- d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- e. Contacting financial institutions and closing or modifying financial accounts; and,
- f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

100. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

101. Further, as a result of Defendant’s conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details

about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

102. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Plaintiff Meeks's Experience

103. Plaintiff Meeks received medical care and assessment resulting in mailings from Defendant in the past. Upon information and belief, he was presented with standard medical forms to complete prior to his service that requested his PII and PHI, including HIPAA and privacy disclosure forms.

104. As part of his assessment and treatment, and as a requirement to receive Defendant's services, Plaintiff Meeks entrusted his PII, PHI, and other confidential information such as name, address, Social Security number, medical and treatment information, and health insurance information to Defendant's customer organization with the reasonable expectation and understanding that Defendant would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to him. Plaintiff would not have used Defendant's customer organization had he known that Defendant would not take reasonable steps to safeguard his Private Information.

105. In late July 2022, months after Defendant learned of the data breach, Plaintiff Meeks received a letter from Defendant, dated July 27, 2022, notifying him that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. The

notice indicated that Plaintiff Meeks's Private Information, including his full name, member ID, and information that may have been provided during a medical health assessment was compromised as a result of the Data Breach.

106. As a result of the Data Breach, Plaintiff Meeks made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach reviewing credit card and financial account statements. He is also researching credit monitoring services to find an affordable option.

107. Plaintiff Meeks has spent a few hours and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

108. Plaintiff Meeks suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Meeks; (b) violation of his privacy rights; (c) the likely theft of his Private Information; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

109. As a result of the Data Breach, Plaintiff Meeks has also suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Meeks is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff also has suffered anxiety about unauthorized parties viewing, using, and/or publishing his information related to his medical records and prescriptions. Plaintiff Meeks is diagnosed with multiple sclerosis and is worried the emotional

distress from this incident could exacerbate his diagnosis.

110. Plaintiff has also experienced a substantial increase in suspicious phishing phone calls, emails, and text messages, which Plaintiff believes is related to his Private Information being placed in the hands of illicit actors.

111. As a result of the Data Breach, Plaintiff Meeks anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Meeks recently suffered a nearly one-hundred point drop in his credit score, to which he has no explanation, and also had to contact his bank as he had unauthorized charges related to a loan that he did not apply for. In addition, Plaintiff Meeks will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

CLASS ACTION ALLEGATIONS

112. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated (“the Class”).

113. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

All persons Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the “Class”).

114. Excluded from the Class are Defendant’s officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

115. Plaintiff reserves the right to amend or modify the Class or Subclass definitions as this case progresses.

116. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately 1,073,316 individuals of Defendant whose sensitive data was compromised in Data Breach.

117. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;
- f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- h. Whether Defendant should have discovered the Data Breach sooner;

- i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant breach implied contracts with Plaintiff and Class Members;
- l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;
- m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;
- n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

118. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

119. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

120. Predominance. Defendant have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

121. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

122. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CAUSES OF ACTION

FIRST COUNT

Negligence

(On Behalf of Plaintiff and the Class)

123. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

124. Plaintiff and Class Members entrusted Defendant with their Private Information.

125. Plaintiff and Class Members entrusted Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and not disclose the Private Information to unauthorized third parties in the ordinary course of mailing services.

126. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members’ Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant’s duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

127. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

128. Defendant’s duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and patients, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

129. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

130. Defendant’s duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

131. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failing to ensure that its email system had plans in place to maintain reasonable data security safeguards;
- d. Failing to have in place mitigation policies and procedures;
- e. Allowing unauthorized access to Class Members' Private Information;
- f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

132. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

133. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

134. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

135. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Breach of Implied Contract
(On behalf of the Plaintiff and the Class)

136. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

137. Plaintiff and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

138. Plaintiff and the Class were required to and delivered their Private Information to Defendant as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

139. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services of Plaintiff and Class Members.

140. In accepting such information and payment for services for customer organizations, Defendant entered into implied contracts with Plaintiff and the other Class Members whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

141. In delivering their Private Information to Defendant's customer organizations and providing payment for healthcare services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the data as part of that service.

142. In their written policies, Defendant expressly and impliedly promised to Plaintiff and Class Members that it would only disclose protected information and other Private Information under certain circumstances, none of which related to a Data Breach as occurred in this matter.

143. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed state law or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

144. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

145. Plaintiff and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

146. Had Defendant disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their Sensitive Information to Defendant.

147. Defendant recognized that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

148. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendant.

149. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

150. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

THIRD COUNT
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

151. Plaintiff repeats and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

152. This count is pleaded in the alternative to Count 2 (breach of implied contract).

153. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant's rendering of medical mailing services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' Personal Information, and by providing Defendant with their valuable Personal Information.

154. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

155. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

156. Defendant acquired the monetary benefit and Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

157. If Plaintiff and Class Members knew that Defendant had not secured their Personal Information, they would not have agreed to provide their Personal Information to Defendant.

158. Plaintiff and Class Members have no adequate remedy at law.

159. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Personal Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Personal Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Personal Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

160. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

161. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FOURTH COUNT
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

162. Plaintiff repeats and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

163. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

164. Defendant owed a duty to Plaintiff and Class Member to keep their Private Information confidential.

165. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' Private Information is highly offensive to a reasonable person.

166. Defendant's reckless and negligent failure to protect Plaintiff and Class Members' Private Information constitutes an intentional interference with Plaintiff and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

167. Defendant's failure to protect Plaintiff's and Class Members' Private Information acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

168. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

169. Because Defendant failed to properly safeguard Plaintiff's and Class Members' Private Information, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

170. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

171. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

172. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiff and the Class.

173. Plaintiff, on behalf of himself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' Private Information.

174. Plaintiff, on behalf of himself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

- a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and his counsel as Class Counsel;
- b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and

Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

- c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;
- d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;
- f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- g) For an award of punitive damages, as allowable by law;
- h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- i) Pre- and post-judgment interest on any amounts awarded; and,
- j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demand a trial by jury of any and all issues in this action so triable as of right.

Dated: August 9, 2022

Respectfully Submitted,

/s/ Joseph M. Lyon
Joseph M. Lyon
THE LYON FIRM, LLC
2754 Erie Ave.

Cincinnati, OH 45208
Tel: 513.381.2333
jlyon@thelyonfirm.com

Terence R. Coates*
Jonathan T. Deters*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jdeters@msdlegal.com

** Pro Hac Vice Forthcoming*

Attorneys for Plaintiff and the Proposed Class